UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/918,062	07/30/2001	Keith Alexander Harrison	30006786-2	2570

7590 12/08/2006

HEWLETT-PACKARD COMPANY
Intellectual Property Administration
P.O. Box 272400
Fort Collins, CO 80527-2400

EXAMINER	
DAVIS, ZACHARY A	
ART UNIT	**PAPER NUMBER**
2137	

DATE MAILED: 12/08/2006

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/918,062	HARRISON ET AL.	
	Examiner	Art Unit	
	Zachary A. Davis	2137	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *24 October 2006*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-19* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-19* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☐ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

Continued Examination Under 37 CFR 1.114

1. A request for continued examination under 37 CFR 1.114, including the fee set forth in 37 CFR 1.17(e), was filed in this application after final rejection. Since this application is eligible for continued examination under 37 CFR 1.114, and the fee set forth in 37 CFR 1.17(e) has been timely paid, the finality of the previous Office action has been withdrawn pursuant to 37 CFR 1.114. Applicant's submission filed on 24 October 2006 has been entered.

2. By the above submission, no claims have been amended, added, or canceled. Claims 1-19 are currently pending in the present application.

Response to Arguments

3. Applicant's arguments with respect to claims 1-19 have been considered but are moot in view of the new ground(s) of rejection.

Examiner's Note

4. The Examiner recommends that care be taken to avoid confusion within the claims between the respective first and second tokens of the sender and intended

recipient. Specifically, it appears that the first and second tokens of the intended recipient have been designated in opposite manners in different groups of claims. That is, in Claims 1-8, the first token of the intended recipient is the private key and the second token of the intended recipient is the corresponding public key, as is explicitly recited in dependent Claim 5 and is clear from the use of the tokens in independent Claim 1, where the second token (i.e. public key) is used for encryption and the first token (i.e. private key) for decoding or decryption; however, in Claims 9-19, it appears that the first token of the intended recipient is instead the public key, and the second token the private key, as is implicit in the use of the tokens in independent Claims 9, 18, and 19, where the first token (assumedly public key) is used for encoding or encryption and the second token (assumedly private key) for decoding or decryption. The Examiner notes that there is no claim within Claims 9-19 that explicitly defines which of the first and second token of the intended recipient is intended to be the public and which the private key, in a manner corresponding to the explicit recitation in Claim 5.

5. The Examiner further notes that the first and second tokens of the sender are clearly defined within all claims; specifically, the first token of the sender is private key and the second token of the sender is the corresponding public key, as explicitly recited in Claims 5 and 17, where the first token is used to encrypt the digest and the second token to decrypt the digest. This is consistent within all groups of claims.

Claim Objections

6. Claim 1 is objected to because of the following informalities:

Due to the (noted) inconsistency noted in the above Examiner's Note, it appears that the limitation in Claim 1, reciting "releasing the document when the intended recipient has proved their identity by use of the second token of the intended recipient that is uniquely related to the first token of the intended recipient", should instead recite "by use of the first token of the intended recipient" and "uniquely related to the second token of the intended recipient"; alternately, the definitions of the first and second tokens of the intended recipient within Claims 1-8 could be reversed so that the definitions are consistent with those in Claims 9-19, or the definitions of the first and second tokens of the intended recipient in Claim 9-19 could be reversed so that the definitions are consistent between all claims.

Appropriate correction is required. For purposes of interpreting the prior art, it will be assumed that the last limitation of Claim 1 recites "by use of the first token of the intended recipient that is uniquely related to the second token of the intended recipient" for simplicity's sake.

Claim Rejections - 35 USC § 103

7. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

8. Claims 1-12 and 14-19 are rejected under 35 U.S.C. 103(a) as being unpatentable over Linsker et al, US Patent 5598473, in view of Mazzagatte et al, US Patent 6862583; Davis et al, US Patent 5633932 (previously cited in the Office action mailed 31 August 2005); and Menezes et al, *Handbook of Applied Cryptography*.

In reference to Claims 1, 5, and 8, Linsker discloses a method for determining the authenticity of a fax document (column 2, lines 23-27) that includes receiving a document and a digest of the document created by a hash algorithm and encrypted with a first token of the sender, which is the sender's private key (column 4, lines 54-60, where digest signature DS is the encrypted digest); obtaining a second token of the sender, which is the sender's public key, relating to the private key (column 4, lines 57-65); decrypting the digest with the public key (column 5, lines 20-23); creating a second digest using a hash algorithm (column 5, lines 23-27, and column 4, lines 25-35); and comparing the decrypted received digest with the second created digest (column 5, lines 23-42). However, although Linsker discloses authenticating the sender of a document, Linsker does not explicitly disclose verifying the identity of the intended recipient of a document.

Mazzagatte discloses a method for authenticated secure printing, which can be implemented for fax documents (column 4, lines 35-37), and which includes receiving and securely retaining a digital document and a transmitted independently verifiable data record of an intended recipient at a printout station (column 8, line 20-column 9,

line 7; noting column 8, line 63-column 9, line 1, where the data is securely stored at the printer; further noting column 8, lines 20-29, where the digital certificate is the independently verifiable data record); obtaining a first token of the intended recipient, which is the recipient's private key (column 4, lines 9-12); requesting proof of the intended recipient's identity at the printout station using the independently verifiable data record (column 9, lines 49-51); and releasing the document when the intended recipient's identity has been proven by use of the first token of the intended recipient that is related to a second token of the recipient, where the second token is the recipient's public key (column 9, lines 46-62). Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the method of Linsker by including verification of the intended recipient in addition to authentication of the sender, in order to ensure that printout of sensitive documents is authorized and that print data is securely stored (see Mazzagatte, column 2, lines 7-10).

Although Linsker discloses authenticating the sender of a document and Mazzagatte discloses verifying the identity of the intended recipient of a document, neither Linsker nor Mazzagatte explicitly discloses that identification data is encrypted specifically by the transmission station. Davis discloses a method for user authentication at a print node, which may process fax documents (see column 1, lines 39-45), and which includes receiving and securely retaining a digital document and a transmitted independently verifiable data record of an intended recipient at a printout station (column 5, lines 13-24; column 6, lines 38-40); obtaining a first token of the intended recipient, which is the recipient's private key (see column 5, lines 52-65);

requesting proof of the intended recipient's identity at the printout station using the independently verifiable data record (column 5, lines 52-65; column 6, lines 40-41); decrypting identifying data with the first token (see column 5, lines 13-18 and 52-65), where the data was encrypted with the second token of the intended recipient, which is the recipient's public key, and the data was encrypted at the transmitting station (column 4, line 39-column 5, line 9, where a header is encrypted at the sending node, where the header can include information identifying the intended recipient); determining the authenticity of the recipient of the document (column 5, line 33-column 6, line 8, noting particularly column 5, lines 52-65 where a private key on a smart card and a challenge/response protocol are used for authentication); and releasing the document when the intended recipient's identity has been proven by use of the first token (column 5, lines 21-24; column 6, lines 41-45). Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the method of Linsker and Mazzagatte by including encryption of identifying data at the transmitting station, in order to allow for confirmation that the intended recipient is present using authentication techniques (see Davis, column 2, lines 26-29, and column 4, lines 65-67).

Although Linsker, Mazzagatte, and Davis disclose that the independently verifiable data record includes identification data (Mazzagatte, column 8, lines 20-30) and that a challenge/response protocol is used to authenticate and prove the intended recipient's identity (Mazzagatte, column 9, lines 58-61; Davis, column 5, lines 58-65), Linsker, Mazzagatte, and Davis do not explicitly disclose that the challenge/response

protocol decrypts encrypted identification data with the recipient's private key, where the identification data was encrypted with the recipient's public key. However, Menezes discloses that challenge-response identification and authentication can be performed based on public-key decryption (page 403, Section 10.3.3, first paragraph). Menezes further discloses that the protocol includes encrypting a challenge, which can be an identifier, with a public key, decrypting the encrypted challenge with a private key to form the response, comparing the challenge and response, and verifying the identity if the comparison result indicates a match (page 404, "(i) Challenge-response based on public-key decryption", noting that, in addition to random numbers, identifier "B" is one of the parts of the challenge). Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the method of Linsker, Mazzagatte, and Davis by implementing the challenge/response protocol in the manner suggested by Menezes, in order to identify the recipient based on its private key (page 403, Section 10.3.3, first paragraph) and avoid chosen text attacks (page 404, paragraph "Identification based on PK decryption and witness").

In reference to Claims 2 and 3, Linsker, Mazzagatte, Davis, and Menezes further disclose receiving a digital certificate of the sender and that the public key is part of the certificate (see Linsker, column 5, lines 2-13).

In reference to Claim 4, Linsker, Mazzagatte, Davis, and Menezes further disclose checking the validity of the certificate online (see Linsker, column 5, lines 6-13).

In reference to Claims 6 and 7, Linsker, Mazzagatte, Davis, and Menezes further disclose printing the document with a verifying mark once it has been authenticated (see Linsker, column 6, lines 3-29).

In reference to Claims 9, 10, and 17, Linsker discloses a method of sending a fax document (column 2, lines 23-27) that includes creating a digest of the document using a hash algorithm (column 4, lines 25-35); encrypting the digest with a first token of the sender, which is the sender's private key (column 4, lines 40-47); obtaining a second token of the sender, specifically the sender's public key, that will be used to decrypt the encrypted digest; and sending the encrypted digest, the document, and the public key to the recipient (column 4, lines 50-53). However, although Linsker discloses authenticating the sender of a document, Linsker does not explicitly disclose verifying the identity of the intended recipient of a document.

Mazzagatte discloses a method for authenticated secure printing, which can be implemented for fax documents (column 4, lines 35-37), and which includes receiving and securely retaining a digital document and a transmitted independently verifiable data record of an intended recipient at a printout station (column 8, line 20-column 9, line 7; noting column 8, line 63-column 9, line1, where the data is securely stored at the printer; further noting column 8, lines 20-29, where the digital certificate is the independently verifiable data record); requesting proof of the intended recipient's identity at the printout station using the independently verifiable data record (column 9, lines 49-51); and releasing the document when the intended recipient's identity has

been proven by use of a second token of the intended recipient that is related to the recipient's first token, where the second token is the recipient's private key (column 9, lines 46-62). Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the method of Linsker by including verification of the intended recipient in addition to authentication of the sender, in order to ensure that printout of sensitive documents is authorized and that print data is securely stored (see Mazzagatte, column 2, lines 7-10).

Although Linsker discloses authenticating the sender of a document and Mazzagatte discloses verifying the identity of the intended recipient of a document, neither Linsker nor Mazzagatte explicitly discloses that identification data is encrypted specifically by the transmission station. Davis discloses a method for user authentication at a print node, which may process fax documents (see column 1, lines 39-45), and which includes obtaining a first token of the intended recipient, which is the recipient's public key (column 3, line 40-column 4, line 56); encrypting identification information of the intended recipient using the first token of the recipient (column 4, line 39-column 5, line 9, where a header is encrypted at the sending node, where the header can include information identifying the intended recipient); sending and then receiving and securely retaining a transmitted document, the encrypted identification information, and a transmitted independently verifiable data record of an intended recipient at a printout station (column 5, lines 13-24; column 6, lines 38-40); requesting proof of the intended recipient's identity at the printout station using the independently verifiable data record (column 5, lines 52-65; column 6, lines 40-41); decrypting

identifying data with a second token, which is the private key of the recipient (see column 5, lines 13-18 and 52-65); determining the authenticity of the recipient of the document (column 5, line 33-column 6, line 8, noting particularly column 5, lines 52-65 where a private key on a smart card and a challenge/response protocol are used for authentication); and releasing the document when the intended recipient's identity has been proven by use of the second token (column 5, lines 21-24; column 6, lines 41-45). Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the method of Linsker and Mazzagatte by including encryption of identifying data at the transmitting station, in order to allow for confirmation that the intended recipient is present using authentication techniques (see Davis, column 2, lines 26-29, and column 4, lines 65-67).

Although Linsker, Mazzagatte, and Davis disclose that the independently verifiable data record includes identification data (Mazzagatte, column 8, lines 20-30) and that a challenge/response protocol is used to authenticate and prove the intended recipient's identity (Mazzagatte, column 9, lines 58-61; Davis, column 5, lines 58-65), Linsker, Mazzagatte, and Davis do not explicitly disclose that the challenge/response protocol decrypts the encrypted identification data with the recipient's private key. However, Menezes discloses that challenge-response identification and authentication can be performed based on public-key decryption (page 403, Section 10.3.3, first paragraph). Menezes further discloses that the protocol includes encrypting a challenge, which can be an identifier, with a public key, decrypting the encrypted challenge with a private key to form the response, comparing the challenge and

response, and verifying the identity if the comparison result indicates a match (page 404, "(i) Challenge-response based on public-key decryption", noting that, in addition to random numbers, identifier "B" is one of the parts of the challenge). Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the method of Linsker, Mazzagatte, and Davis by implementing the challenge/response protocol in the manner suggested by Menezes, in order to identify the recipient based on its private key (page 403, Section 10.3.3, first paragraph) and avoid chosen text attacks (page 404, paragraph "Identification based on PK decryption and witness").

In reference to Claims 11 and 12, Linsker, Mazzagatte, Davis, and Menezes further disclose proving the sender's identity by transferring data from a personal portable data carrier holding the private key to the transmission station from which the document will be sent, and that the sender enters a verifiable security identifier to establish the sender's identity (see Linsker, column 7, lines 13-21).

In reference to Claims 14-16, Linsker, Mazzagatte, Davis, and Menezes further disclose obtaining details of the sender, including the public key, from a central database, and providing the details and public key in a digital certificate (see Linsker, column 4, lines 50-53; column 5, lines 2-13).

Claims 18 and 19 are apparatus claims corresponding substantially to the methods of Claims 1 and 9, and are rejected by a similar rationale.

9. Claim 13 is rejected under 35 U.S.C. 103(a) as being unpatentable over Linsker in view of Mazzagatte, Davis, and Menezes as applied to claim 11 above, and further in view of Clark, US Patent 5448045.

Linsker, Mazzagatte, Davis, and Menezes disclose everything as applied above in reference to Claim 11. However, Linsker, Mazzagatte, Davis, and Menezes do not explicitly disclose that the digest is encrypted within the personal portable data carrier. Clark discloses that digital signatures (formed by encrypting a message digest with a private key) can be performed in smart cards (column 8, lines 53-58). Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the method of Linsker, Mazzagatte, Davis, and Menezes to include encrypting the digest within the personal portable data carrier, in order to prevent compromise of the sender's private key (see Clark, column 8, lines 57-62).

Conclusion

10. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

a. The Examiner again notes that Chan et al, US Patent 6378070, previously cited in the Office action mailed 31 August 2005, discloses a method for secure printing that verifies that the intended recipient is the only one able to print a secure document, where information necessary for decryption is encrypted at the sending node using the intended recipient's public key, and the intended

recipient is authenticated at the printing node using a smart card storing the corresponding private key.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Zachary A. Davis whose telephone number is (571) 272-3870. The examiner can normally be reached on weekdays 8:30-6:00, alternate Fridays off.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Emmanuel Moise can be reached on (571) 272-3865. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

ZAD
zad

EMMANUEL L. MOISE
SUPERVISORY PATENT EXAMINER